

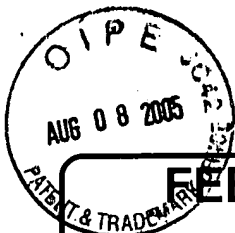
1 AE
\$ 2134
JFW

TRANSMITTAL FORM (to be used for all correspondence after initial filing)		Application No.	10/028,894
		Filing Date	December 17, 2001
		First Named Inventor	David W. Grawrock
		Art Unit	2134
		Examiner Name	David Yiuk Jung
Total Number of Pages in This Submission	6	Attorney Docket Number	42390P13483

ENCLOSURES (check all that apply)		
<input checked="" type="checkbox"/> Fee Transmittal Form <input checked="" type="checkbox"/> Fee Attached <input type="checkbox"/> Amendment / Response <input type="checkbox"/> After Final <input type="checkbox"/> Affidavits/declaration(s) <input type="checkbox"/> Extension of Time Request <input type="checkbox"/> Express Abandonment Request <input type="checkbox"/> Information Disclosure Statement <input type="checkbox"/> PTO/SB/08 <input type="checkbox"/> Certified Copy of Priority Document(s) <input type="checkbox"/> Response to Missing Parts/Incomplete Application <input type="checkbox"/> Basic Filing Fee <input type="checkbox"/> Declaration/POA <input type="checkbox"/> Response to Missing Parts under 37 CFR 1.52 or 1.53	<input type="checkbox"/> Drawing(s) <input type="checkbox"/> Licensing-related Papers <input type="checkbox"/> Petition <input type="checkbox"/> Petition to Convert a Provisional Application <input type="checkbox"/> Power of Attorney, Revocation Change of Correspondence Address <input type="checkbox"/> Terminal Disclaimer <input type="checkbox"/> Request for Refund <input type="checkbox"/> CD, Number of CD(s)	<input type="checkbox"/> After Allowance Communication to Group <input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences <input checked="" type="checkbox"/> Appeal Communication to Group (Appeal Notice, Brief, Reply Brief) <input type="checkbox"/> Proprietary Information <input type="checkbox"/> Status Letter <input checked="" type="checkbox"/> Other Enclosure(s) (please identify below): <div style="border: 1px solid black; padding: 5px; margin-top: 5px;">- Check in the amt of \$500.00 - Return Receipt Postcard</div>
Remarks		

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT	
Firm or Individual name	Paul A. Mendonsa, Reg. No. 42,879 BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Signature	
Date	June 10, 2005

CERTIFICATE OF MAILING/TRANSMISSION			
I hereby certify that this correspondence is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.			
Typed or printed name	Rachael L. Brown		
Signature		Date	August 5, 2005



FEE TRANSMITTAL for FY 2005

Patent fees are subject to annual revision.

Complete if Known

☐ Applicant claims small entity status. See 37 CFR 1.27.

TOTAL AMOUNT OF PAYMENT (\$)

500.00

Application Number	10/028,894
Filing Date	December 17, 2001
First Named Inventor	David W. Grawrock
Examiner Name	David Yiuk Jung
Art Unit	2134
Attorney Docket No.	42390P13483

METHOD OF PAYMENT (check all that apply)

☒ Check ☐ Credit card ☐ Money Order ☐ None ☐ Other (please identify):

☐ Deposit Account Deposit Account Number: Deposit Account Name: Blakely, Sokoloff, Taylor & Zafman LLP

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☐ Charge fee(s) indicated below

☐ Charge fee(s) indicated below, except for the filing fee

☒ Charge any additional fee(s) or underpayment of fee(s) under 37 CFR §§ 1.16, 1.17, 1.18 and 1.20. ☒ Credit any overpayments

FEE CALCULATION

1. EXTRA CLAIM FEES

Total Claims	Extra Claims	Fee from below	Fee Paid
Independent Claims	20* = 0	50.00	\$0.00
Multiple Dependent	3* = 0	200.00	\$0.00

Large Entity

Fee Code	Fee (\$)	Fee Code	Fee (\$)	Fee Description
1202	50	2202	25	Claims in excess of 20
1201	200	2201	100	Independent claims in excess of 3
1203	360	2203	180	Multiple Dependent claim, if not paid
1204	300	2204	150	**Reissue independent claims over original patent
1205	300	2205	150	**Reissue claims in excess of 20 and over original patent

SUBTOTAL (1) (\$)

0.00

**or number previously paid, if greater, For Reissues, see below

2. ADDITIONAL FEES

Large Entity

Fee Code	Fee (\$)	Fee Code	Fee (\$)	Fee Description
1051	130	2051	65	Surcharge - late filing fee or oath
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet
2053	130	2053	130	Non-English specification
1251	120	2251	60	Extension for reply within first month
1252	450	2252	225	Extension for reply within second month
1253	1,020	2253	510	Extension for reply within third month
1254	1,590	2254	795	Extension for reply within fourth month
1255	2,160	2255	1,080	Extension for reply within fifth month
1401	500	2401	250	Notice of Appeal
1402	500	2402	250	Filing a brief in support of an appeal
1403	1,000	2403	500	Request for oral hearing
1451	1,510	2451	1,510	Petition to institute a public use proceeding
1460	130	2460	130	Petitions to the Commissioner
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)
1806	180	1806	180	Submission of Information Disclosure Stmt
1809	790	1809	395	Filing a submission after final rejection (37 CFR § 1.129(a))
1810	790	2810	395	For each additional invention to be examined (37 CFR § 1.129(b))

Other fee (specify)

SUBTOTAL (2)

Fee Paid

500.00

(\$)

500.00

SUBMITTED BY

Complete (if applicable)

Name (Print/Type) Paul A. Mendonsa

Registration No. 42,879
(Attorney/Agent)

Telephone (503) 439-8778

Signature

Date

08/05/05



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:

David W. Grawrock for
Intel Corporation

Serial No.: 10/028,894

Group Art Unit: 2134

Filed: December 17, 2001

Examiner: David Yiuk Jung

FOR: CONNECTING A VIRTUAL TOKEN TO A PHYSICAL TOKEN

08/09/2005 SHASSEN1 00000012 10028894

01 FC:1402

500.00 DP

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicant (hereinafter Appellant) submits this appeal brief, thus perfecting the notice of appeal filed on June 10, 2005.

The required headings and subject matter follow.

(i) Real party in interest.

This case is assigned of record to Intel Corporation, who is the real party in interest.

(ii) Related appeals and interferences.

There are no known related appeals and / or interferences.

(iii) Status of claims.

Claims 1-30 are pending in the case, and claims 1-30 stand rejected. The rejection of claims 1-30 is being appealed.

(iv) Status of amendments.

No amendments were filed subsequent to the final rejection.

(v) Summary of claimed subject matter.

Paragraph numbering of the filed application and the published application may differ. Accordingly, the following description references paragraphs of the present application based upon the paragraph numbering of the application as published on June 19, 2003. Further, supplied reference numbers and paragraphs are not meant to limit the scope of the present claims but merely to provide examples of some elements to aid understanding. The actually claim scope may be broader and/or more narrow than the example elements given.

Claim 1 relates to a method that comprises receiving a certification message CertM1 (See, paragraphs [0043]-[0046]) generated by a physical token 150 (See, FIGS. 1-2 and paragraphs [0017]-[0022]) of a computing device 100. The certification message CertM1 attests to a public key 262 or 272 (See, FIG. 2) associated with a virtual token 160 (See, FIGS. 1-2, paragraphs [0023]-[0024]) of the computing device 100 and the physical token 150. Claim 1 further relates to requesting an entity 195 and to issue a credential (e.g. VT endorsement credential) for the public key 262 associated with the virtual token 160 based upon the certification message CertM1. See, paragraphs [0033]-[0035] for an explanation of the process used by a certificate authority to issue an identity credential to a physical token. See, FIG. 4 and

related disclosure for details regarding a process used to issue an endorsement credential for a virtual token.

Claim 8 relates to a physical token 150 for a computing device 100. The physical token 150 comprises a register 240, 242, and/or 244 to record an integrity metric that measures a virtual token 160 of the computing device 100. The physical token 150 further comprises one or more processing units 210 to generate a random number Nonce1 and a certification message CertM1 that specifies the register 240, 242, 244 that is encrypted by a key CAPub of an entity 195, and that has uniqueness based upon the random number Nonce1. See, paragraphs [0020], [0030], [0043]-[0045].

Claim 13 relates to a computing device 100 comprising a virtual token 160, a physical token 150, and a processor 110. The virtual token 160 records integrity metrics. The physical token 150 records an integrity metric that measures the virtual token 160, and generates a certification message CertM1 that attests to the integrity metric, that is encrypted by an asymmetric key CAPub of an entity 195, and that has uniqueness. The processor 110 requests the entity 195 to issue a credential (VT endorsement credential) for an asymmetric key 260, 262, 270, 272 associated with the virtual token 160 based upon the certification message CertM1.

Claim 17 relates to a computing device comprising a physical token 150 and a virtual machine monitor 310. The physical token 150 generates a certification message CertM1 that attests to an operating environment 300 of the computing device 100 and a credential (PT identity credential) issued to the physical token 150. The virtual machine monitor 310 comprises a virtual token 160 to further attest to the operating environment 300. The virtual machine monitor 310 requests the physical token 150 to provide the certification message CertM1 and causes the certification message CertM1 to be transferred to an entity 195. The virtual machine

monitor 310 further receives a credential (VT endorsement credential) for the virtual token 160 in response to transferring the certification message CertM1 to the entity 195.

Claim 22 relates to a method that comprises receiving a request for a credential (VT endorsement credential) to be issued to a virtual token 160 of a computing device 100. (See, block 430, paragraph [0053]). Claim 22 further relates to determining whether the virtual token 160 satisfies criteria for a suitable virtual token based upon information of the request. (See, block 438, 446, 450, 454, 458 and paragraphs [0055]-[0060]). Claim 22 further relates to issuing the credential (VT endorsement credential) to the virtual token 160 of the computing device 100 in response to determining that the virtual token 160 satisfies the criteria. (See, block 462 and paragraph [0061]).

Claim 26 relates a machine readable medium comprising instructions, which in response to being executed, result in a computing device 100 generating a certification message CertM1 that attests to a physical token 160 and an operating environment 300 of a computing device 100. The instructions further result in the computing device 100 requesting that an entity 195 issue a credential (VT endorsement credential) to a virtual token 160 of the computing device 100 based upon the certification message CertM1.

(vi) Grounds of rejection to be reviewed on appeal.

Claims 1-30 stand rejected under 35 U.S.C. § 103(a), as being unpatentable over admitted prior art (APA) and Gong et al.

(vii) Argument.

The rejection of claims 1-30 under 35 U.S.C. § 103(e), as being unpatentable over admitted prior art (APA) and Gong is in error and should be reversed.

It is well established that obviousness requires a teaching or a suggestion by the relied upon prior art of all the elements of a claim (M.P.E.P. §2142). Without conceding the appropriateness of the combination, Appellant respectfully submits that the combination of the APA and Gong does not meet the requirements of an obvious rejection in that neither teaches nor suggests a “virtual token” as required by claims 1-30.

It appears that the Official Action is relying on the APA for a teaching or suggestion of a “virtual token.” The Background section of Appellant’s application describes aspects of a Trust Platform Module (TPM) such as the TPM described in the Trusted Platform Computing Alliance (TPCA) Main Specification, Version 1.1, 31 July 2001. Further, the Background section clearly identifies the TPM as a “physical token”. In short, the Appellant’s Background section and the Trusted Platform Computing Alliance Main Specification merely provide a teaching of a “physical token” and do not teach or suggest a “virtual token” as required by claims 1-30.

Appellant pointed out in a response filed September 7, 2004 that neither the Background section of Appellant’s application nor the cited Gong reference teach a virtual token. Further, the Appellant respectfully requested the Examiner to provide with more specificity where “virtual token” was taught in Gong or the APA. In the Official Action mailed March 11, 2005, the Examiner pointed to FIG. 2 of Appellant’s application as the only support for a teaching of a “virtual token.” FIG. 2 does in fact disclose a virtual token 160 as well as FIG. 1 and a large portion of Appellant’s “Detailed Description.” The problem is that FIG. 2 and the portions of the

“Detailed Description” that accompany FIG. 2 are descriptions of Appellant’s own invention and are not admitted prior art.

The Examiner has provided no specific indication as to what in Appellant’s application the Examiner is treating as admitted prior art. Appellant noted the lack of clarity in their response filed on September 7, 2004 and indicated that the Appellant was operating under the assumption that the Examiner was referring solely to the Background section of Appellant’s application as admitted prior art. However, in light of the latest Official Action, it appears the Examiner is using the description of Appellant’s own invention to provide a teaching of “virtual token” and is thus not basing the present rejection merely on that which is found in the prior art. As stated above, it is well established that obviousness requires a teaching or a suggestion by the relied upon prior art of all the elements of a claim (M.P.E.P. §2142). Since the present rejection is not based solely on the prior art but relies on the description of Appellant’s invention for a teaching of a virtual token, the Examiner has failed to present a prima facie case of obviousness in regards to claims 1-30. Appellant respectfully requests the rejection of claims 1-30 be reversed.

CONCLUSION

In view of the foregoing, favorable reconsideration and reversal of the rejections is respectfully requested. Early notification of the same is earnestly solicited. If there are any questions regarding the present application, the Examiner and / or the Board is invited to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,

Aug 5, 2005
Date

Paul A. Mendonsa
Paul A. Mendonsa
Reg. No. 42,879
(503) 439-8778

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313 on.

8/5/05
Date of Deposit
Rachael Brown
Name of Person Mailing Correspondence
[Signature] 8/5/05
Signature Date

(viii) Claims appendix.

1. (Original) A method comprising
receiving a certification message generated by a physical token of a computing device that attests to a public key associated with a virtual token of the computing device and the physical token; and
requesting an entity to issue a credential for the public key associated with the virtual token based upon the certification message.
2. (Original) The method of claim 1 wherein receiving comprises
receiving the certification message that is encrypted by a public key of the entity and that comprises a hash of both the public key associated with the virtual token and a credential issued to the physical token.
3. (Original) The method of claim 2 wherein requesting comprises
sending to the entity the certification message, the public key associated with the virtual token, and the credential issued to the physical token.
4. (Original) The method of claim 3 wherein requesting further comprises
sending to the entity one or more integrity metric quotes from the physical token and one or more logs associated with the integrity metric quotes.

5. (Original) The method of claim 1 further comprising
encrypting one or more integrity metric quotes with a session key of a symmetric
cryptographic algorithm to obtain a first encrypted parameter;
encrypting the certification message and session key with a public key associated with
the entity to obtain a second encrypted parameter;
wherein requesting comprises sending to the entity the first encrypted parameter and the
second encrypted parameter.

6. (Original) The method of claim 1 wherein receiving comprises
receiving the certification message encrypted by the public key of the entity, the
certification message comprising a hash that attests to the public key associated with the virtual
token and a credential issued to the physical token.

7. (Original) The method of claim 1 wherein receiving comprises
receiving the certification message encrypted by the public key of the entity, the
certification message comprising the public key associated with the virtual token and a credential
issued to the physical token.

8. (Original) A physical token for a computing device, comprising
a register to record an integrity metric that measures a virtual token of the computing
device, and
one or more processing units to generate a random number and a certification message
that specifies the register, that is encrypted by a key of an entity, and that has uniqueness based
upon the random number.

9. (Original) The physical token of claim 8 wherein
the one or more processing units generates the certification message such that the
certification message further comprises a hash that identifies a key associated with the virtual
token and a credential issued to the physical token.

10. (Original) The physical token of claim 8 wherein
the one or more processing units generates the certification message such that the
certification message further identifies a key associated with the virtual token and a credential
issued to the physical token.

11. (Original) The physical token of claim 8 wherein
the integrity metric comprises a hash of a virtual machine monitor that comprises the
virtual token.

12. (Original) The physical token of claim 8 wherein
the certification message comprises one or more hashes that attest to a key associated with the virtual token, the credential issued to the physical token, and an index specifying the register.

13. (Original) A computing device comprising
a virtual token to record integrity metrics;
a physical token to record an integrity metric that measures the virtual token, and to generate a certification message that attests to the integrity metric, that is encrypted by an asymmetric key of an entity, and that has uniqueness; and
a processor to request the entity to issue a credential for an asymmetric key associated with the virtual token based upon the certification message.

14. (Original) The computing device of claim 13 wherein
the physical token generates the certification message such that the certification message that identifies the asymmetric key associated with the virtual token and a credential issued to the physical token, and
the processor sends the entity the certification message, the asymmetric key associated with the virtual token, and the credential issued to the physical token.

15. (Original) The computing device of claim 14 wherein
the processor further sends one or more integrity metric quotes from the physical token and one or more logs associated with the integrity metric quotes.

16. (Original) The computing device of claim 13 wherein the processor sends the entity a symmetric key that is encrypted with the asymmetric key of the entity, and sends the entity the certification message, the asymmetric key associated with the virtual token, and the credential issued to the physical token that are encrypted with the symmetric key.

17. (Original) A computing device comprising a physical token to generate a certification message that attests to an operating environment of the computing device and a credential issued to the physical token; and a virtual machine monitor comprising a virtual token to further attest to the operating environment, wherein the virtual machine monitor requests the physical token to provide the certification message, causes the certification message to be transferred to an entity, and receives a credential for the virtual token in response to transferring the certification message to the entity.

18. (Original) The computing device of claim 17 wherein the physical token generates the certification message such that the certification message further comprises one or more hashes that identify a public key associated with the virtual token and the credential issued to the physical token.

19. (Original) The computing device of claim 17 wherein
the physical token generates the certification message such that the certification message
further comprises a public key associated with the virtual token and the credential issued to the
physical token.

20. (Original) The computing device of claim 17 wherein
the physical token generates the certification message to include an integrity metric
representative of the virtual machine monitor.

21. (Original) The computing device of claim 17 wherein
the physical token and virtual token attest to the operating environment by providing
quotes of recorded integrity metrics, and
the virtual machine monitor further provides the entity with one or more quotes of
recorded integrity metrics.

22. (Original) A method comprising
receiving a request for a credential to be issued to a virtual token of a computing device;
determining whether the virtual token satisfies criteria for a suitable virtual token based
upon information of the request; and
issuing the credential to the virtual token of the computing device in response to
determining that the virtual token satisfies the criteria.

23. (Original) The method of claim 22 wherein determining comprises analyzing a credential provided by the request that was issued to a physical token of the computing device.

24. (Original) The method of claim 23 wherein determining further comprises analyzing an integrity metric representative of the virtual token of the computing device.

25. (Original) The method of claim 24 wherein determining further comprises analyzing an integrity metric that is based upon a hash of a monitor that comprises the virtual token.

26. (Original) A machine readable medium comprising instructions, which in response to being executed, result in a computing device
generating a certification message that attests to a physical token and an operating environment of a computing device; and
requesting that an entity issue a credential to a virtual token of the computing device based upon the certification message.

27. (Original) The machine readable medium of claim 26 wherein the instructions, in response to being executed, further result in the computing device
generating the certification message such that the certification message comprises a hash that attests to a public key associated with the virtual token.

28. (Original) The machine readable medium of claim 27 wherein the instructions, in response to being executed, further result in the computing device

generating the certification message such that the certification message is encrypted by a public key of the entity and the hash further attests to a credential issued to the physical token.

29. (Original) The machine readable medium of claim 28 wherein the instructions, in response to being executed, further result in the computing device

sending the public key associated with the virtual token and the credential associated with the physical token.

30. (Original) The machine readable medium of claim 26 wherein the instructions, in response to being executed, further result in the computing device

generating the certification message such that the certification message is encrypted with a public key of the entity and comprises one or more hashes that attest to a public key associated with the virtual token and the credential associated with the physical token;

encrypting the public key associated with the virtual token, the credential associated with the physical tokens, the certification message, quotes of integrity metrics recorded by the physical token, and logs associated with the integrity metrics with a session key to obtain a first parameter; and

encrypting the session key with the public key of the entity to obtain a second parameter, wherein requesting comprises sending the entity the first parameter and the second parameter.

(ix) Evidence appendix.

None.

(x) Related proceedings appendix.

None.